

HP Virtual Connect Manager Version 1.20

Release Notes and Compatibility Matrix



Part Number 467891-001
November 2007 (First Edition)

© Copyright 2007 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Audience assumptions

This document is for the person who installs, administers, and troubleshoots servers and storage systems. HP assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

About this document

These release notes provide information that supersedes the information in the documentation set released with version 1.20 of Virtual Connect Manager.

Contents

- Hardware and firmware requirements 4
 - HP Virtual Connect Manager firmware 4
 - Supported hardware 4
 - Firmware upgrade requirements 5
 - Recommended firmware versions for this release 5
 - HP Virtual Connect Fibre Channel Module Compatibility Matrix 6
- New features 8
- Important notes and recommendations 10
- Known issues 12
 - General 12
 - Fibre Channel and SAN boot 13
 - User interface 13
 - Firmware update 14
- Resolved issues 16

Hardware and firmware requirements

HP Virtual Connect Manager firmware

The latest HP Virtual Connect Manager firmware package (version 1.20) contains the following firmware versions:

- HP 1/10Gb VC-Enet version 1.20
- HP 4Gb VC-FC version 1.10



IMPORTANT: The VC-Enet module firmware must be updated to version 1.20 before updating the VC-FC module firmware. Otherwise, the VC-FC firmware might not appear to be successfully updated.

Supported hardware

Version 1.20 of HP Virtual Connect firmware supports the following hardware:

- Virtual Connect modules
 - HP 1/10Gb Virtual Connect Ethernet Module
 - HP 1/10Gb-F Virtual Connect Ethernet Module
 - HP 4Gb Virtual Connect Fibre Channel Module
- Server blades and workstation blades
 - HP ProLiant BL460c Server Blade
 - HP ProLiant BL480c Server Blade
 - HP ProLiant BL465c Server Blade
 - HP ProLiant BL680c G5 Server Blade
 - HP ProLiant BL685c Server Blade
 - HP ProLiant xw460c Blade Workstation (only the two embedded Ethernet ports are supported; Ethernet and Fibre Channel mezzanine cards are not supported)
- Enclosures
 - HP BladeSystem c-Class c7000 Enclosure with Onboard Administrator
 - HP BladeSystem c-Class c3000 Enclosure with Onboard Administrator
- Integrated Network Interfaces and mezzanine cards
 - HP BladeSystem Dual NC370i Multifunction Network Adapter
 - HP NC373i Integrated Multifunction Gigabit Server Adapter
 - HP NC373m PCI Express Dual Port Multifunction Gigabit Server Adapter
 - HP NC326i Integrated Dual Port PCI Express Gigabit Server Adapter

- HP NC326m PCI Express Dual Port Multifunction Gigabit Server Adapter
- HP NC325m PCI Express Quad Port Gigabit Server Adapter
- HP QLogic QMH2462 4Gb FC HBA for c-Class BladeSystem
- HP Emulex LPe1105-HP 4Gb FC HBA for c-Class BladeSystem

For the latest list of supported hardware, see the HP website (<http://www.hp.com/go/bladesystemupdates>).

Firmware upgrade requirements



IMPORTANT: For optimal operation of HP Virtual Connect Manager, use the recommended firmware versions.

Install the recommended firmware for the following items:

- Server blade system ROMs
- Ethernet mezzanines
- Fibre Channel mezzanines
- HP BladeSystem Onboard Administrator

For additional information on recommended firmware versions and to download firmware upgrades, see the HP website (<http://www.hp.com/go/bladesystemupdates>).

Recommended firmware versions for this release

Product	Recommended firmware version	Minimum firmware version
HP Onboard Administrator	<ul style="list-style-type: none"> • For c7000 enclosures, version 2.02a or later • For c3000 enclosures, version 2.04 or later 	<ul style="list-style-type: none"> • For c7000 enclosures, version 1.30 or later • For c3000 enclosures, version 2.04 or later
iLO	Version 1.35 or later	—
BL460c and BL480c	System ROM 2007.06.28 or later	—
BL465c and BL685c	System ROM 2007.04.05 or later	—
xw460c	System ROM 2007.04.03 Rev A or later	—
BL680c G5	System ROM 2007.08.09 or later	—
BL860c	System, BMC and iLO-2 version 1.01A	—
NC370i, NC373i, and NC373m	<p>Boot code version 1.9.6 and C Class option ROM 1.1.3* or later</p> <p>To use NC373m with the BL680c G5 server blade, the option ROM must be updated to NC373m Boot code version 1.9.6 and C Class option ROM 1.2.7 or later.</p>	—

Product	Recommended firmware version	Minimum firmware version
NC326i, NC325m, and NC326m	<p>Boot code version 3.28 and C Class option ROM 1.1.3* or later</p> <p>To use NC325m with the BL680c G5 server blade, the option ROM must be updated to NC325m Boot code version 3.28 and C Class option ROM 1.2.8 or later.</p> <p>To use NC326m with the BL680c G5 server blade, the option ROM must be updated to NC326m Boot code version 3.28 and C Class option ROM 1.2.8 or later.</p>	—
QLogic QMH2462 4Gb FC HBA	<p>For ProLiant server blades, use QLogic multiboot image 1.63 (with BIOS 1.26) or later.</p> <p>For Integrity server blades use EFI 1.09 (in Multiboot 1.64) or later</p>	—
HP Emulex LPe 1105-HP 4Gb FC	Emulex boot-pair 6.00a2 and 3.2a1 HBAnywhere or later	—

* Use the HP Gigabit Server Adapter Firmware Upgrade Utility for c-Class Blades version 1.10 (HP website (<http://h18023.www1.hp.com/support/files/server/us/download/25604.html>)) or one of the online methods available for the OS. To find the online update method for your OS, go to the HP website (<http://www.hp.com/go/bladeupdates>) and search for Server Blade Software & Updates.

Version 1.20 of HP Virtual Connect firmware checks the server ROM image version and displays an incompatible state only for server blades that have a VC Server Profile assigned and are using incompatible server ROM versions. No version checking of mezzanine card firmware is available, so be sure to verify that the mezzanine card firmware is up-to-date.

Server blades and mezzanine cards that do not meet the required firmware versions do not properly accept Virtual Connect-assigned parameters (MACs, WWNs, and so on), and therefore maintain factory defaults. However, these server blades do have the Ethernet network and Fibre Channel fabric connectivity specified in their Virtual Connect server profiles. This connectivity enables the use of network-based firmware update tools to update server blade and mezzanine firmware.

HP Virtual Connect Fibre Channel Module Compatibility Matrix

The following table lists the switches and firmware versions that are supported with HP Virtual Connect Fibre Channel interconnect modules.

Switch family	Supported versions	Unsupported switches
Brocade and HP B-series Fibre Channel switches	<p>FOS 5.2.1b, 5.3.0</p> <p>FOS 5.1.0d</p>	<ul style="list-style-type: none"> • Brocade 4/12 SAN Switch for c-Class • Brocade 4/24 SAN Switch for c-Class • HP MSA SAN switches • HP StorageWorks 2/8 EL and 2/16 EL switches

Switch family	Supported versions	Unsupported switches
McData and HP M-series Fibre Channel switches	E/OS 9.03.00 E/OS 9.00.00 E/OS 8.02.00	<ul style="list-style-type: none"> • McDATA Intrepid 10000 Director switch
Cisco and HP C-series Fibre Channel switches	SAN-OS 3.1(2a), 3.1(2b), 3.1(3a)	<ul style="list-style-type: none"> • Cisco MDS 9124e Fabric Switch for c-Class • Cisco MDS 9124 Fabric Switch • Cisco MDS 9020 Fabric Switch

New features

The VC-Enet version 1.20 firmware includes the following features:

- HP BladeSystem c-Class c3000 Enclosure support
- HP ProLiant BL680c G5 Server Blade support
- HP ProLiant xw460c Blade Workstation support
- Command line interface for Virtual Connect Manager

The CLI enables administrators to manage a Virtual Connect Domain configuration using the command line, either interactively at the SSH login console or by using a script. The CLI provides the commonly used VC management capabilities that are currently provided through the VC Manager GUI.

- Automated firmware updates

A single command for firmware updates of all VC modules is included in the GUI and the CLI. This optional update method eliminates the user interaction required during the activation step of the firmware update process.

- LDAP support

LDAP uses Directory services to authenticate user credentials and roles. VC domains configured with LDAP can authenticate users in the LDAP directory, so that a user's password or roles can be modified across multiple VC domains by changing one central directory.

- SNMP support

SNMP enables network management tools to monitor the overall state of the VC domain (Ok, degraded, failed, unintegrated) in an unauthenticated manner.

- Port monitoring

This feature enables users to mirror the traffic of any server blade port (up to 16 ports) within the domain to an available uplink port so that an external network analyzer can be connected. The feature provides the ability to configure any uplink port as the analyzer port, and includes a visual indication that the uplink is configured as a mirror port.

- IGMP Snooping

In the GUI and CLI the user can enable or disable IGMP snooping on a per domain basis to restrict multicast packets to those ports participating in the multicast group. VC Manager v1.20 supports IGMP v1 and v2. IGMP v3 is not supported in the current release.

- Show Stacking Link State

With this enhancement, the overall VC domain status reflects stacking link status. Connectivity and redundancy status for stacking links are reflected in the overall domain status.

- Administrative module removal

This feature enables removal of unused modules from the VC domain without 'missing module' indications. The feature is supported when the module uplinks are not configured for use (VC-Enet) or fabrics are not in use by server profiles (VC-FC).

- Support for Multiple Users
Multiple users are allowed within multiple VC Manager windows.
- Support for longer passwords
Password length has been extended to 39 characters.
- Separate MAC and PXE assignments
Previously, PXE support was associated with VC assigned MAC addresses. This feature enables the user to control PXE settings even if they are not using VC assigned MACs. PXE settings for each server profile now include "Enabled", "Disabled", or "Use BIOS".
- VCM reset command
This feature provides a method to reset and reinitialize the VC Manager without affecting server connectivity to Ethernet networks. Using the force option causes a failover.

For additional information, see the Virtual Connect user guide on the HP website (<http://www.hp.com/go/bladeSystem/documentation>).

Important notes and recommendations

When a c-Class enclosure is used with Virtual Connect v1.20, the following configuration restrictions and guidelines apply:

- Plan your interconnect module usage carefully before running the Virtual Connect Domain Setup Wizard. After an interconnect bay is configured for use with a Virtual Connect Ethernet module or VC-FC module, it remains configured for that module type until the overall VC domain is deleted. Virtual Connect reports failures for any VC-Enet or VC-FC module that is removed from the domain.
- Ensure that all Virtual Connect Ethernet and VC-FC modules in a VC domain are at the same firmware revision. To check the firmware revision level, select the "Firmware Update" tab on the "Domain Settings" page. The firmware revision level for each module in the domain is shown.
- To help ensure proper operation after firmware updates, clear the browser cache and reload the browser.
- Only connect HP 4Gb VC-FC Module uplinks to Fibre Channel switch ports that are NPIV-enabled. If using a Brocade FC switch, verify that NPIV is properly enabled by using the `portshow` command. If not properly enabled, you might need to downgrade the Brocade switch firmware, and then upgrade the firmware again for the enable to work properly.
- Always install a Virtual Connect Ethernet module in interconnect bay 1.
- For redundancy, HP recommends installing a second Virtual Connect Ethernet module in interconnect bay 2.
- For c7000 enclosure interconnect bays 3-8, install a Virtual Connect Ethernet module or HP 4Gb VC-FC Module in the bay corresponding to the mezzanine signals.
- Verify that all system component firmware is up to date. A server blade is displayed as incompatible by Virtual Connect Manager if the server ROM is not at the minimum level required by Virtual Connect. Virtual Connect Manager is not able to verify firmware revisions for all components, so a server blade component can be incompatible even if the server blade is not listed as incompatible.
- To improve network performance and prevent unnecessary Spanning Tree Topology Change Notifications (TCN) on the network, configure Ethernet switches connected to Virtual Connect with the same Spanning Tree settings you would use when connecting to a server blade NIC. For Cisco switches, this is done by using the `portfast` command to enable ports connected to a VC-Enet module. This action ensures that link state changes on Virtual Connect do not cause a TCN.
- Do not use Virtual Connect and non-Virtual Connect modules in horizontally adjacent bays.
- Virtual Connect Manager assigns or migrates MAC addresses or WWNs for server Ethernet and FC ports connected to HP Virtual Connect modules. Virtual Connect Manager also assigns MAC addresses and WWNs to server Ethernet or FC ports that are not connected to an I/O module because Virtual Connect modules can be added later. Server Ethernet and FC ports connected to non-Virtual Connect modules retain the server factory default MACs addresses and WWNs.
- Verify that all iLOs and Virtual Connect modules have valid and unique IP addresses on the same subnet as the OA. Without IP addresses on all modules, Virtual Connect does not work properly.

- Back up the Virtual Connect domain configuration each time changes are made. While saved in non-volatile memory and check-pointed to the neighboring module, HP recommends saving the configuration external to the enclosure.
- Removing a VC-Enet module and plugging it into another enclosure causes the configuration information on that module to be cleared. This action prevents a configured spare from overwriting configuration data in another enclosure.
- HP 1/10Gb VC-Enet modules support 10GBASE-CX4 stacking cables 0.5 m to 7 m (1.64 ft to 23.00 ft). The 1000BASE-T links can also be used as stacking links of up to 100 m (328 ft). When multiple cables of either the same or dissimilar type (for example 1Gb and 10Gb) are connected to the same two modules, they are aggregated to provide enhanced throughput for the stacking link.
The CX4 interface uses the same physical connector as Infiniband, but Infiniband cables are tuned differently and will not perform as well in CX4 applications. HP recommends purchasing CX4 cable assemblies that meet the IEEE CX4 specifications and support 10-Gigabit communication at distances from 3 m to 15 m (9.84 ft to 49.20 ft).
- The Onboard Administrator must have an IP address on the same subnet as the Virtual Connect module before the administrator sets the Enclosure Bay IP Addressing (EBIPA) mode. Changing the EBIPA address for a module causes the module to be reset by the OA (resulting in an outage) when the change is applied. If multiple modules have their EBIPA address changed, all modules experience the outage at approximately the same time.
- The port monitoring network analyzer port should only be connected directly to an analyzer. Improper connection of the port or improper configuration of the port monitoring could result in network loops and cause a network outage.
- Port monitoring is disabled in a mixed firmware environment. If any module in the domain is running a version of firmware prior to v1.20, port monitoring is automatically disabled.
- When the management network is fully saturated, access to the VC Manager and response times might be slower due to network congestion.

For additional information, see the Virtual Connect user guide on the HP website (<http://www.hp.com/go/bladeSystem/documentation>).

Known issues

General

- For configuration changes, the VC Manager can take up to 90 seconds for the new information to be saved to non-volatile storage. Configuration information might be lost if power is removed during this update time.
- When an SSH key is uploaded using the GUI interface, user authentication fails. The user must enter the password when logging in using SSH.
- The VC Manager CLI `set ldap` command `IpAddress` option supports only an IP address. This command option does not support the DNS name of the directory server as stated in the Command Line help and CLI user guide.
- The VC Manager domain configuration database in v1.20 is not downward compatible with previous versions, causing an issue when downgrading from v1.20 or in an environment where the primary and secondary VC Managers are at different firmware levels.

For example, if a primary VC Manager is running v1.20 and a secondary VCM is running 1.16, the primary VC Manager check-points the domain configuration (in v1.20 format) to the secondary VC Manager. If a failover causes the secondary VC Manager to become the primary, it is unable to initialize because it cannot interpret the v1.20 configuration file. Avoid running different firmware versions on the primary and secondary modules in an enclosure.

- Virtual Connect modules with firmware revisions of v1.00 and v1.10 are not compatible and cannot be upgraded within the c3000 enclosure. Modules must be upgraded in a c7000 enclosure, or contact your HP representative for additional options. Virtual Connect modules with v1.15 and v1.16 in a c3000 enclosure should be upgraded to v1.20 for full support of the c3000 enclosure.
- When updating the VC Manager firmware, the prompt for file downloads to a local system might be blocked by the browser security setting.
- During an Onboard Administrator failover, Virtual Connect Manager can lose communication with the Onboard Administrator for as long as 15 minutes. During this time, Virtual Connect Manager is not able to make profile changes to server blades or perform some enclosure administration functions, such as powering server blades on and off.
- When operating in a redundant Onboard Administrator environment and the user requests a "Transition Standby to Active" to the standby Onboard Administrator, then communication between the Virtual Connect Manager and the active Onboard Administrator might be lost. To restore communication, reset the Virtual Connect Manager (Tools->Reset Virtual Connect Manager).
- Replacing the OA in an enclosure containing only one OA causes the OA to lose all of the Virtual Connect configuration for the server blades. Server blades configured for VC-assigned MAC addresses or WWNs are marked as "Profile Pending." Rebooting a server blade after replacing the OA causes it to revert to the factory default MAC addresses. The user must re-enter the OA user name and password to restart the VC Mode. Replacing a redundant OA does not result in this situation.

- If an enclosure import is attempted with a server blade in a failed state, the Virtual Connect Manager might report an erroneous error. If the import completes, close the browser and log in again to verify the import was successful. The working state of all server blades can be verified using the Onboard Administrator.
- Changes in the server ROM-based setup utilities (RBSU) can override Virtual Connect server profile settings for PXE (enabled or disabled). If a change is made in RBSU, that change is not reflected in Virtual Connect Manager. If PXE is set through RBSU, HP recommends using the "Use BIOS" setting.
- RDP "rip and replace" does not work properly when using VC-administered MAC addresses because RDP is tracking the server blades by MAC address rather than by the primary lookup key (which can be set to serial number, MAC address, UID, or Asset Tag). To work around this issue, manually redeploy the server blade.
- For VC-Enet modules, do not use the Get-Bulk feature with SNMPv2c MIB walk. The MIB walk operation halts prematurely before running through the entire MIB. When using SNMPv2c protocol for MIB walk make sure that the Get-Bulk option is not enabled.
- The SNMP agent on VC-Enet modules does not validate the read community string. The agent responds to SNMP GET requests with any community string. To inhibit the agent discovery the SNMP agent must be disabled.
- When scripting CLI commands, only a single scripting client should perform remote management operations to a remote Virtual Connect Manager. If multiple scripting clients are used to perform a heavy load of CLI commands to a single Virtual Connect Manager, some management commands might fail, and in some cases, the primary module might need to be reset to properly recover.

Fibre Channel and SAN boot

- The VC-Enet module firmware must be updated before the VC-FC module firmware. Otherwise, the VC-FC firmware might not appear to be successfully updated.
- To properly boot from SAN with some versions of Linux and VMware ESX 3.0.1, change the QLogic HBA connection options to "point to point only" in the QLogic BIOS configuration utility.
- Virtual Connect Manager does not provide an interface to force 1-Gb speed on the VC-FC module uplink and downlink ports. However, the ports will auto-negotiate properly to 1 Gb.
- The Fibre Channel login sequence can be delayed by approximately 20 seconds when more than one server blade HBA is aggregated through the same VC-FC uplink port attached to a Cisco switch and these HBAs are in the same zone. To avoid this problem, do not place server HBAs in the same zone on the fabric switch.
- When configuring Trap Destination IP addresses for the VC-FC modules, be sure that trap destinations are capable of supporting SNMPv2 type traps.
- The number of SNMP trap destination addresses is limited to one trap destination for VC-FC modules.

User interface

- Virtual Connect Manager allows users to change the number of VC-FC Module uplink ports connected to an external Fabric Switch without a warning while a server might be accessing remote storage devices.

- Virtual Connect Manager shows either a server blade or an interconnect module as degraded (but not both) for an I/O Ekey mismatch.
- Network uplinks that are linked after the Network Setup Wizard has been started may not show proper link status in the wizard. When the wizard is completed, all uplink link statuses are displayed correctly.
- A server profile can be assigned to a device bay with a server that has fewer physical NIC ports than defined in the server profile. In most cases, a warning is provided, but in some cases it is not.
- If a server is rebooted several times while its server profile is being edited, an error displaying an XSL transformation failure may be displayed. Do not edit a server profile while repeatedly rebooting a server.
- In the Bay Summary screen for a VC-FC module in Virtual Connect Manager, some servers might be displayed with the incorrect model number. The model number is displayed correctly in other screens and in the Onboard Administrator.
- In the Server Connections tab of the Ethernet Networks screen, the port status shows OK even if the server port is not linked.

Firmware update

- The VC-Enet module firmware must be updated before the VC-FC module firmware. Otherwise, the VC-FC firmware might not appear to be successfully updated.
- If the firmware update procedure indicates a failure to activate a module or appears to be stuck, it might be caused by a timeout and/or a stale web page. To refresh the screen and verify the actual update status, click the **Firmware update** link under Domain Settings in the left navigation pane of the VCM user interface.
- During the firmware update activation countdown, an Internet Explorer pop-up might be displayed stating "Failed to create processor object: The stylesheet does not contain a document element. The stylesheet may be empty, or it may not be a well-formed XML document." This pop-up can be dismissed without consequences.
- After a firmware update, clear the browser cache. If the browser cache is not cleared after a firmware update, VC Manager might not function properly.
- Aborted uploads of firmware images remain in the /upload/ folder and can eventually fill up the space. The GUI might report an "unknown error" or format error. To recover from this error, force a failover of the primary VC Manager.
- After a firmware update from v1.15 or v1.16 to v1.20, the fabrics associated with the Fibre Channel uplinks might show a failed state even though the uplinks are still linked and functional. To resolve this condition, select the fabric from the GUI left panel, change the uplink port speed to a new setting, and then change the fabric uplink speed to the original setting. This action activates the Apply button. Click **Apply** and the fabric state is recalculated to the correct state.
- The Virtual Connect v1.20 automated firmware update might not complete the firmware installation on the VC-FC modules aligned with the primary VC Ethernet module. To complete the firmware update, do one of the following:
 - If a temporary fabric outage is acceptable, issue a reset to the modules using the Onboard Administrator.
 - Manually restart the firmware update on the VC-FC modules, and no outage occurs.

- While executing individual (not automated) firmware updates, the Update button might appear after clicking the Activate button for a VC-Enet module.
 - Ignore the Update button if it persists for more than 3 minutes. If the Update button appears for more than 3 minutes, then the firmware update failed and should be re-attempted.
 - If the Update button is clicked in this state, it reports an error in installation. This error can be ignored.
- During automated firmware update, if the primary VC module is running the same or a higher version than the selected firmware update package, and the "Allow firmware downgrades and/or re-update" check-box is *not* selected, then only modules with lower firmware than the selected package are updated. Upon completion of any updates, the firmware update page might display inaccurate version numbers. To correct the display, select the "Firmware management" link in the left navigation pane.

Resolved issues

The following issues that existed in Virtual Connect v1.16 have been resolved in Virtual Connect v1.20:

- The Virtual Connect Manager now recovers from a dual-OA failover or the replacement of a single OA without requiring a reset of the Virtual Connect Manager.
- Under certain fail-over conditions a loop could be caused for a very short window (up to about 120 mS). This time was sufficient for BPDUs to slip through and BPDUguard to run.
- VC-FC Port operational and speed statuses reflected configuration settings rather than actual port status information.
- VC-FC module no longer presents "Link to Management URL" in the OA graphical interface because web-based management is not available.
- VC-FC module now supports SNMP and SMI-S management interfaces in read-only mode.
- VC-FC corrected an issue with Non-Disruptive Code Load and Activation when all 16 server blades were logged in to the Fibre Channel SAN.
- If non-Administrator credentials were entered for the Onboard Administrator during Virtual Connect Domain Import, the import failed without explanation.